KEY PROVISIONS FROM AR 380-5

Section VII
Corrective Actions and Sanctions

1–20. General
Commanders will establish procedures to make sure that prompt and appropriate action is taken concerning a violation of the provisions of this regulation, especially in those cases involving incidents which can put classified information at risk of compromise, unauthorized disclosure, or improper classification of information. Such actions will focus on a correction or elimination of the conditions that caused or contributed to the incident.

1–21. Sanctions
a. DA personnel will be subject to sanctions if they knowingly, willfully, or negligently—
(1) Disclose classified or sensitive information to unauthorized persons.
(2) Classify or continue the classification of information in violation of this regulation.
(3) Violate any other provision of this regulation.

b. Sanctions can include, but are not limited to warning, reprimand, suspension without pay, forfeiture of pay, removal, discharge, loss or denial of access to classified information, and removal of original classification authority. Action can also be taken under the Uniform Code of Military Justice (UCMJ) for violations of that Code and under applicable criminal law, if warranted.

c. Original classification authority will be withdrawn for individuals who demonstrate a disregard or pattern of error in applying the classification and sensitivity standards of this regulation.

Section V
Sensitive Information (Computer Security Act of 1987)
5–19. Description
a. The Computer Security Act of 1987 established requirements for protection of certain information in federal government Automated Information Systems (AIS). This information is referred to as "sensitive" information, defined in the Act as: "Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, USC (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy."

b. Two aspects of this definition deserve attention. First, the Computer Security Act of 1987 applies only to unclassified information which deserves protection. Second, unlike most other programs for protection of information, the Computer Security Act of 1987 is concerned with protecting the availability and integrity, as well as, the confidentiality of information. Much of the information which fits the Computer Security Act of 1987's definition of "sensitive" falls within the other categories of information discussed in this chapter.

3.0. Definitions
3.1. "Caveated" information is information subject to one of the authorized control markings under section 9.

3.2. Intelligence Community (and agencies within the Intelligence Community) refers to the United States Government agencies and organizations and activities identified in section 3 of the National Security Act of 1947, as amended, 50 USC 401a(4), and section 3.4(f) (1 through 6) of Executive Order 12333.

3.3. Intelligence information and related materials (hereinafter referred to as "Intelligence") include the following information, whether written or in any other medium, classified pursuant to EO 12958 or any predecessor or successor Executive Order.